UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/405,031	09/24/1999	DOUGLAS R. COFFLAND	IL-10360	9034

7590 11/23/2007

LLOYD E DAKIN JR
ASSISTANT LABORATORY COUNSEL
LAWRENCE LIVERMORE NATIONAL LABORATORY
P O BOX 808-L-703
LIVERMORE, CA 94551

EXAMINER	
BETIT, JACOB F	

ART UNIT	PAPER NUMBER
2164	

MAIL DATE	DELIVERY MODE
11/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/405,031	COFFLAND, DOUGLAS R.	
	Examiner	Art Unit	
	Jacob F. Bétit	2164	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 September 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/7/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Remarks

1. In response to communications filed on 7 September 2007 claims 1-30 are presently pending in the application.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

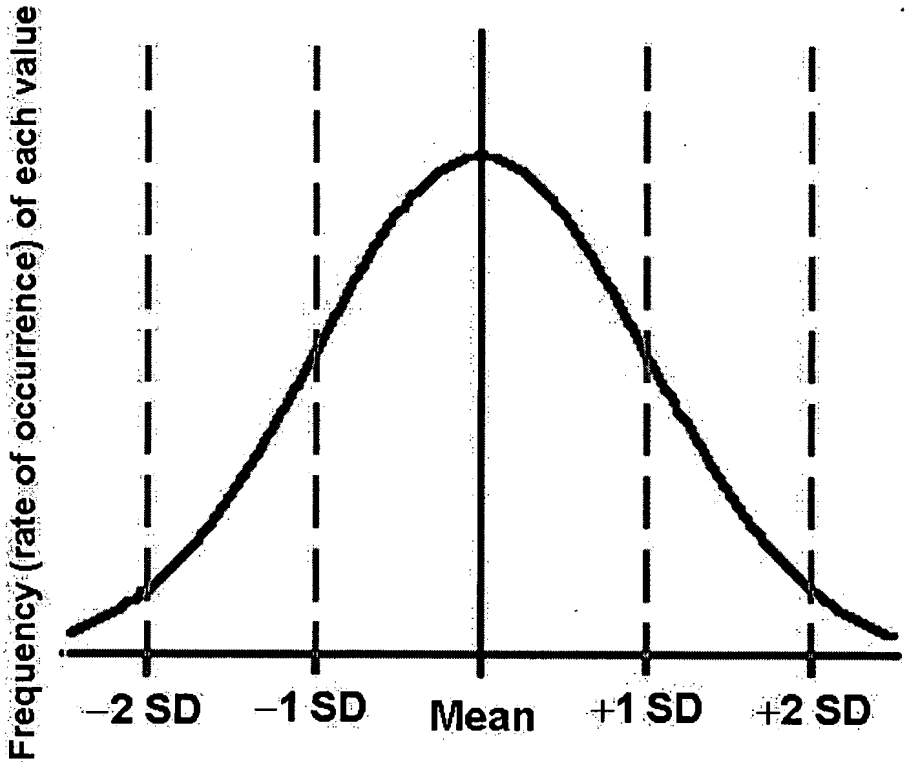
> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1-30 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claims 1, 10, 17, and 24 recite limitation "random noise being unpredictable from one moment to the next". This limitation is not described in the specification in such a way as to reasonably convey to one skilled in the relevant art, at the time the application was filed, had possession of the claimed invention. The specification states, "in one embodiment of the present invention, the media signal need only include random transducer noise having a noise signal amplitude". One example of how this can be done is "a lens-cap could be on the camera causing the scene to be perfectly quiescent." By putting the lens-cap on the camera the signal becomes more predictable, not "unpredictable" as claimed by the applicant. This is because the output of

the camera signal when capturing a chaotic signal has two somewhat unpredictable signals added together to make a more unpredictable signal (i.e., $Chaotic_{SIGNAL} + Noise_{signal} = Signal$). The chaotic signal has more effect on the change in the quantized sample because the amplitude of a camera is going to have a much higher signal for the image captured by the camera than the noise produced by the camera. The chaotic signal would change several quantization levels when the image being captured is changed whereas if the quantization levels of the camera were set at a level close to the amplitude of the noise, as suggested by the specification, the quantized sample would only vary slightly (1-2 quantization levels) from the chaotic signal being captured. Therefore if the chaotic signal was replaced with a predictable signal by putting the lens-cap on, the resulting signal would be more predictable than before because the only changing data in the signal would be the noise from the transducer (camera), which only varies by a few quantization levels.

The random noise that is part of the claimed media signal is "white Gaussian noise" as disclosed in the specification. This noise is not "unpredictable" as claimed by the applicant because Gaussian noise is predictable based on the Gaussian Curve an example of which is shown below.



The graph shows that values that are closer to the mean are more likely to occur over time than values further away from the mean. Therefore "white Gaussian noise" is not "unpredictable" as currently recited in the claims.

The specification states, "Thus, even a perfectly quiescent media signal 104 (e.g., when a lens cap is on a video camera containing the transducer 102) will contain *some randomness* from the transducer noise." The applicant's specification then states, "Put another way, as long as a size of a smallest quantizer step is no larger than an amplitude of the transducer 102 noise, the quantized media signal 108 will include a *high level* of randomness even if input to the transducer is perfectly quiescent." The applicant does not disclose: the steps required to go from "some randomness" to "high level of randomness"; and from "high level of randomness" the steps required to go to "random noise only" and being "unpredictable".

Further proof that the media signal disclosed in the specification does not contain data that is "unpredictable" is the compression and hashing steps that following the acquisition of the signal that is claimed to be "unpredictable". These steps as disclosed by the specification are used to reduce the predictability of the keyword generated. The compressed data stream is used to remove redundant data strings so that only differences between data frames are presented, and because frames of a compressed media signal can vary in size, sets of data can easily be taken from different parts of the frames, helping to limit the amount of redundant data collected. The hashing step is used because it "assures that the resultant identifier 311 varies significantly even if the set of data 309 only varies by one bit." If the data that was acquired originally was completely random and unpredictable, there would be no reason to go through these steps.

Claims 2-9, 11-16, 18-23, and 25-30 are rejected for depending on independent claims 1, 10, 17, and 24.

4. Claims 1-30 are rejected under 35 U.S.C. 112, first paragraph, as based on a disclosure which is not enabling. Multimedia encryption critical or essential to the practice of the invention, but not included in the claim(s) is not enabled by the disclosure. See *In re Mayhew*, 527 F.2d 1229, 188 USPQ 356 (CCPA 1976). The preamble of claims 1 and 17 state "a system adapted for use for multimedia encryption". The preamble of claim 10 states "a method adapted for use for multimedia encryption". The preamble for claim 24 states "a computer-usable medium embodying computer program code adapted for use for multimedia encryption". Both the specification and the claims disclose steps for producing a keyword which could be used as a key for encryption or a key for generating pseudo-random numbers that are later used in

encryption, however, neither the specification nor the claims disclose any steps, elements or instructions that encrypt multimedia.

Claims 2-9, 11-16, 18-23, and 25-30 are rejected for depending on independent claims 1, 10, 17, and 24.

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1-30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. Claims 1-30 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, elements or instructions. See MPEP § 2172.01. The preamble of claims 1 and 17 state "a system adapted for use for multimedia encryption". The preamble of claim 10 states "a method adapted for use for multimedia encryption". The preamble for claim 24 states "a computer-usable medium embodying computer program code adapted for use for multimedia encryption". However the steps, elements, or instructions of the claims disclose creating a keyword. The claims omit the steps, elements, or instructions of actually encrypting any multimedia data.

Claims 2-9, 11-16, 18-23, and 25-30 are rejected for depending on independent claims 1, 10, 17, and 24 and for omitting the same steps, elements, or instructions that the independent claims omit.

Response to Arguments

8. Applicant's arguments filed on 7 September 2007 have been fully considered but they are not persuasive.

In response to the applicant's arguments directed towards the 35 USC § 112 first paragraph rejection given above on the grounds that the limitation "random noise being completely unpredictable from one moment to the next", the arguments have been fully considered but are not deemed persuasive. While it is not argued that the specification does state that the noise is "completely unpredictable", it is argued that the specification does not state where a reliable source for this noise is. The specification does disclose white Gaussian noise as giving the signal "**some randomness**" not that it makes the signal completely unpredictable. This **Gaussian noise** is then **added** to the **chaotic signal** to produce a signal that is harder to predict than the chaotic signal alone. If the applicant was to **amend the claims** so that they were directed towards adding **a white Gaussian noise signal to a chaotic signal**, the applicant **would be accurately describing** what is disclosed in the specification.

In response to the applicant's amendments meant to fix the rejections in numbered paragraph 5 of the previous office action, the amendments fail to make multimedia encryption part of the claim and fail to show how the original specification supports steps of making multimedia encryption part of the claim. The amendments also fail to remove multimedia encryption as the intended use of the claim. The applicant appears to be **creating a keyword for use in encryption** and does not appear to be encrypting anything. Therefore the claims are not for use for multimedia encryption, as stated, rather **for generating a keyword** that can be used in

any of several types of encryption including multimedia encryption. If the applicant was to amend the claim 1 to recite **"A system for generating a keyword that can be used in multimedia encryption"**, claim 10 to recite **"A method for generating a keyword that can be used in multimedia encryption"**, claim 17 to recite **"A system for generating a keyword that can be used in multimedia encryption"**, and claim 24 to recite **"A computer-useable medium embodying computer program code for generating a keyword that can be used in multimedia encryption"**; the preambles of the claim would more closely resemble what is being described in the applicant's specification.

The claim steps **do not encrypt multimedia** because the steps envolved in the claim make it **impossible for multimedia to be decrypted** at a later time. A **hash** by definition is a **one-way algorithm**, and therefore it would be not be possible to decrypt the keyword to retrieve the data set.

In response to the applicant's arguments directed towards the rejection under 35 USC §101, the rejection has been withdrawn, and therefore they are moot.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jacob F. Betit whose telephone number is (571) 272-4075. The examiner can normally be reached on Monday through Friday 9:30 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Charles Rones can be reached on (571) 272-4085. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

jfb
19 Nov 2007

C. Rones

CHARLES RONES
SUPERVISORY PATENT EXAMINER